COSO Revised: Implications for Compliance and Ethics Programs

Urton Anderson, CCEP
Director of the Von Allmen School of Accountancy and EY Professor
The University of Kentucky

Session Agenda
- The COSO Framework – beyond internal control over financial reporting
- What changed, why, and implications for ethics and compliance.
- Principle 1 – demonstrating a commitment to integrity and ethical values
- Compliance Objectives and the 17 Principles
- The 17 Principles and the elements of an effective compliance program
- Implementation Issues – the experience from year 1
- The future of COSO as a framework for compliance and ethics

The COSO Framework

Beyond internal control over financial reporting
- Framework for compliance
  Internal Control is a process, effected by an entity's board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:
  - Effectiveness and efficiency of operations.
  - Reliability of financial reporting.
  - Compliance with applicable laws and regulations.
  COSO
The COSO Framework

The original 1992 COSO Framework
- Definition of Internal Control
- Five-component framework
- Objective driven

Compliance Example

The COSO Framework Revised – What Changed

2013 Revision
- Same 5 components
- 17 Principles
- Points of Focus
Points of Focus – Principle 2

2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

- Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.

- Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate actions.

Key Linkages

- Objectives
- Risks
- 5 components of Effective IC
- Risks Relate to Objectives
- 17 Principles
- Points of Focus

17 Principles

<table>
<thead>
<tr>
<th>Control Environment</th>
<th>Risk Assessment</th>
<th>Control Activities</th>
<th>Information and Communication</th>
<th>Monitoring Activities</th>
</tr>
</thead>
</table>

Must be Articulated and Measurable

Risks Relate to Objectives

5 components of Effective IC

Points of Focus
Points of Focus – Principle 2

• Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

• Provides Oversight for the System of Internal Control—The board of directors retains oversight responsibility for management’s design, implementation, and conduct of internal control:
  - Control
  - Risk Assessment
  - Control Activities
  - Information and Communication
  - Monitoring

The COSO Framework Revised – Why

▪ Changes in nature of organizational governance
▪ Change in technology
▪ Change in organizational relationships (extended enterprises, 3rd party risk, strategic alliances)
▪ Increased reporting requirements for ICFR

The COSO Framework Revised – Implication for Compliance

▪ Increased emphasis on compliance objectives
▪ Move focus on control activities to principles in the control environment
  ▪ Principle 1
Principle 1

The organization demonstrates a commitment to integrity and ethical values.

Points of Focus - Principle 1

- Sets the Tone at the Top
- Establishes Standards of Conduct
- Evaluates Adherence to Standards of Conduct
- Addresses Deviations in a Timely Manner

Evaluation of Principle 1

Three aspects to Principle 1

- Overall Effectiveness of IC
  - Direct entity-level controls
- Effectiveness of IC for compliance risks (Compliance)
  - Direct entity-level controls
- Required for SOX 404 for effectiveness of IC over financial reporting (ICFR)
  - Indirect entity-level controls
Evaluation of Principle 1

- Required for SOX 404 for effectiveness of IC over financial reporting (ICFR)
  - Indirect entity-level controls
  - Would a defect in the presence or function of this principle indicate that there is a reasonable possibility of a material misstatement of the f/s?
- In 404 external auditor begins with management’s self assessment and then possibly testing related indirect key controls.

Evaluation of Principle 1

Approaches

- Evaluation of the ethical culture of the organization
- Evaluation of compliance program effectiveness (7 elements)
- Evaluation of compliance system maturity

Compliance Objectives and the 17 Principles

- What are compliance objectives?
  examples
  - To establish and promote a culture of integrity, compliance, competence and accountability; doing the right thing.
  - We do not discriminate at any level of the organization on the basis of race, gender, age, religious beliefs or any other legally protected characteristic.
  - Alcatel-Lucent has a zero-tolerance policy for compliance violations and reinforces full integrity in every business action from every employee.
17 Principles

Control Environment | Risk Assessment | Control Activities | Information and Communication | Monitoring Activities
2. Establishes oversight responsibilities 4. Identifies and analyzes significant changes 10. Identifies and evaluates the potential impact of change 14. Communicates effectively
3. Establishes structure, authority, and responsibility 5. Assesses key risk areas 11. Identifies and evaluates any potential use of new or emerging technologies 15. Communicates externally
4. Demonstrates commitment to competence 6. Identifies and analyzes possible risk scenarios 12. Deploys through policies and procedures
5. Demonstrates knowledge, understanding, and commitment to ethical behavior 7. Assess and compares information 13. Communicates information to appropriate parties

Seven Elements for Effective Ethics and Compliance Program

1. Establish Policies, Procedures and Controls
2. Exercise Effective Compliance and Ethics Oversight
3. Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals
4. Communicate and Educate Employees on Compliance and Ethics Programs
5. Monitor and Audit Compliance and Ethics Programs for Effectiveness
6. Ensure Consistent Enforcement and Discipline of Violations
7. Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents
8. Conduct ongoing risk assessment

Linking the 7 Elements and the COSO Principles

1. Establish Policies, Procedures and Controls
- 1. Demonstrates commitment to integrity and ethical values
- 2. Exercises oversight responsibility

2. Exercise Effective Compliance and Ethics Oversight
- 2. Exercises oversight responsibility
- 3. Establishes structure, authority and responsibility

3. Exercise Due Diligence to Avoid Delegation of Authority to Unethical Individuals
- 4. Demonstrates commitment to competence
Linking the 7 Elements and the COSO Principles

4. Communicate and Educate Employees on Compliance and Ethics Programs

• 14. Communicates internally

5. Monitor and Audit Compliance and Ethics Programs

• 14. Conducts ongoing or separate evaluations
• 16. Identifies and analyzes significant change

6. Ensure Consistent Enforcement and Discipline of Violations

• 15. Enforces accountability

7. Respond Appropriately to Incidents and Take Steps to Prevent Future Incidents

• 17. Evaluates and communicates deficiencies

8. Conduct ongoing risk assessment

• 6. Specifies relevant objectives
• 7. Identifies and analyzes risk
• 10. Selects and develops control activities

Implementation Issues – the experience from year 1

- Key control activities versus principles and points of focus
- Difficulty of relating principles to key controls (many principles indirect entity level controls)
- 404 reviews still focused on key controls – principles management self assessment
The future of COSO as a framework for compliance and ethics

- Principle 1 – broadens scope of ICFR reviews
- The objective-risk-control-monitor process is an effective basis for managing compliance risk
- Integration risk management framework – COSO ERM revision

Ultimately for COSO Internal Control - Assurance that risk are being managed to an appropriate level
- The demand by board members and senior management for this assurance continues to increase – primarily for assurance on compliance risks
- New extensions
  - 3 Lines of Defense Model
  - Combined Assurance

Organization as a Web of Assurance
COMBINED ASSURANCE

King III
Principle 3.5
The audit committee should ensure that a combined assurance model is applied to provide a coordinated approach to all assurance activities.

Assurance Map (PWC)
Questions?

Urton Anderson
Von Allmen School of Accountancy
The University of Kentucky
(859)218-1788
urton.anderson@uky.edu